JOURNAL OF ALGEBRA 91, 281–293 (1984)

Mock Covers and Galois Extensions

DAVID HARBATER*

Department of Mathematics, University of Pennsylvania, Philadelphia, Pennsylvania 19104

Communicated by Walter Feit

Received January 3, 1983

In [Hal], the notion of mock cover was used in order to construct tamely ramified Galois coverings of curves, with desired group and branching data. There the curves were defined over an algebraically closed field, and so coverings of a given curve could be obtained via specialization, once an algebraic family of such covers was constructed. Here the technique is exploited to construct formal families of Galois coverings of more general curves. This yields Galois extensions of power series rings. In the case of curves over fields, the formal family may be constructed so as to descend to an algebraic family. If the ground field is algebraically closed of characteristic p, we again may specialize, and can obtain Galois coverings with desired "purely wild" ramification (subject to the condition that the ramification generates the Galois group). In the arithmetic case, we show that all finite groups occur over $\mathbb{Z}[[t]]$, and also over its subring $\mathbb{Z}_{r+}[[t]]$ of power series holomorphic on $|t| \leqslant r$. That construction uses local data obtained using techniques of [Sa]; the patching and deformation use results of [Ha3].

We will use the following terminology: Let T be a domain and $S \supset T$ a finitely generated T-algebra such that no non-zero element of T is a zero divisor in S. The total ring of fractions of S may thus be regarded as an extension of the fraction field of T. If this latter extension is separable, call $T \subset S$ a *generically separable* extension. If in addition S is finite over T, call $\operatorname{Spec} S \to \operatorname{Spec} T$ a *cover*. Given a finite group G, a *G-Galois cover* (or simply *G-cover*) consists of such a cover together with a group homomorphism $G \to \operatorname{Aut}_T S$ which induces a simply transitive action of G on a generic geometric fibre. Call the cover (and the corresponding extension) *Galois* with group G if in addition S is a domain; in this case G is the full automorphism group of S over T.

* Supported in part by the NSF.

0021-8693/84 $3.00

1. Mock Covers and the Geometric Case

We will consider a technique of building covers (and extensions) from simpler ones, by means of patching. Each of the patches, and the resulting cover, will have a degenerate fibre, called a "mock cover."

Let X be a reduced and irreducible scheme, and $Z \to^{\pi} X$ a finite morphism whose restriction to each irreducible component of Z is an isomorphism onto Z. Then $Z \to^{\pi} X$ is called a *mock cover*, and the irreducible components are its *sheets*. A mock cover is in particular generically separable. If a finite group G acts on Z over X, then $Z \to X$ together with the action of G is G-Galois provided that G acts simply transitively on each unramified fibre, or equivalently on the sheets.

1.1. Proposition. *Suppose $Z \to X$ is a G-Galois mock cover of curves, and that Z_0 is a sheet. Then Z is connected if and only if G is generated by the stabilizers of the ramified points on Z_0.*

Proof. Let $a_1, \ldots, a_n \in X$ be the branch points, and let G_i be the stabilizer of the point on Z_0 above a_i. Thus Z_0 meets $\gamma(Z_0)$ over a_i if and only if $\gamma \in G_i$, and so $\delta(Z_0)$ meets $\delta\gamma(Z_0)$ over a_i if and only if $\gamma \in G_i$.

Now Z is connected if and only if for every sheet $\delta(Z_0)$ there is a sequence of sheets

$$Z_0, Z_1, \ldots, Z_m = \delta(Z_0)$$

such that Z_{i-1} meets Z_i over some a_{j_i}, for $1 \leqslant i \leqslant m$. Write $Z_i = \delta_i(Z_0)$. Then Z_{i-1} meets Z_i over a_{j_i} if and only if the element $\gamma_i = \delta_{i-1}^{-1}\delta_i$ lies in G_{j_i}. Thus Z is connected if and only if for every $\delta \in G$ there are integers $1 \leqslant j_1, \ldots, j_m \leqslant n$ and elements $\gamma_i \in G_{j_i}$ $(1 \leqslant i \leqslant m)$ such that $\gamma_1 \cdots \gamma_m = \delta$. This is equivalent to asserting that the subgroups G_i generate G. ∎

Given extensions $A \subset S \subset T$ with A algebraically closed in S, call $S \subset T$ a *regular* extension of A-algebras if A is algebraically closed in T as well. Thus in order that a cover of $\operatorname{Spec} A[[t]]$ be regular (i.e., the corresponding extension is), it is sufficient that the fibre over $(t = 0)$ be a mock cover.

1.2. Proposition. *Let G be a finite group and $H_1, \ldots, H_m \subset G$ subgroups which generate G. Let A be a Dedekind domain and $f_1, \ldots, f_m \in A$ non-zero elements which generate the unit ideal of A. Write $A_i = A[f_i^{-1}]$, $U_i = \operatorname{Spec} A_i$. Let $A_i[[t]] \subset E_i$ be a Galois extension with group H_i. Suppose that the fibre over $(t = 0)$ of $Z_i = \operatorname{Spec} E_i$ is a mock cover $Z_i^0 \to \operatorname{Spec} A_i$, and that Z_i^0 is unramified over $U_i \cap U_j$, for $j \neq i$. Then there is a unique Galois cover $Z \to X = \operatorname{Spec} A[[t]]$ with group G, whose fibre over $X_i = \operatorname{Spec} A_i[[t]]$ agrees (as a G-cover) with the disjoint union $Z_i^{\amalg(G:H_i)}$.*

Here $(G: H_i)$ is the index of H_i in G.

Proof. The disjoint union $Z_i^{\amalg(G:H_i)}$ can be made into a (disconnected) G-cover of X_i by choosing a base point on each copy of Z_i and choosing a corresponding set of left coset representatives for H_i in G. Thus the sheets are labelled by the elements of G, and $g \in G$ takes the "identity sheet" of Z_i^0 to the sheet labelled by g.

Now for $i \neq j$, the pullback of $Z_i^{\amalg(G:H_i)}$ over $A[f_i^{-1}f_j^{-1}][[t]]$ is a trivial G-cover, and the same is true over $A[f_i^{-1}f_j^{-1}, t]/(t^v)$. So the corresponding rings $E_i^{(G:H_i)}$ $(i = 1,..., m)$ induce, for each $v \geqslant 1$, a coherent sheaf of G-algebras over $\operatorname{Spec} A[t]/(t^v)$. We thus obtain a compatible system of G-algebras over the rings $A[t]/(t^v)$, for $v \geqslant 1$. Passing to the inverse limit yields a G-algebra E over $A[[t]]$. Let $Z = \operatorname{Spec} E$. Thus $Z \to X$ agrees with Z_i over X_i. So $Z \to X$ is a cover, whose fibre over $(t = 0)$ is a mock cover (being generically trivial).

It remains to show that Z is irreducible, or equivalently that its normalization $\tilde{Z}$ is connected. Let $\tilde{Z}_i$ be the normalization of Z_i. By 1.1, the identity sheet over $(t = 0)$ of the G-Galois cover $\tilde{Z}_i^{\amalg(G:H_i)}$ intersects the sheets labelled by the elements of some generating set of H_i. Since Z agrees with $Z_i^{\amalg(G:H_i)}$ over U_i, and since the H_i generate G, Z is connected by 1.1. ∎

Remark. Suppose that the Dedekind domain A is of transcendence degree 1 over a field k, and that Z_i (in 1.2) arises as the pullback of a cover of $\operatorname{Spec} A[t]$ (or more generally of $\operatorname{Spec} A \times_k C$, where C is a curve of finite type over k). Then there is an étale neighborhood (Y, y) of the origin in the t-line $\mathbb{A}_k^1$ (resp. of a point in C) and a Galois cover $W \to \operatorname{Spec} A \times_k Y$ with group G, whose formal completion at $\operatorname{Spec} A \times_k \{y\}$ is $Z \to \operatorname{Spec} A[[t]]$. This follows from Theorem 4.2 of [Hal], applied to the smooth completion of $\operatorname{Spec} A$.

1.3. COROLLARY. *Let A be a Dedekind domain. Let S be the set of positive integers n such that for every non-zero $f \in A$, there is a cyclic degree n Galois cover of* $\operatorname{Spec} A[f^{-1}][[t]]$ *whose fibre over $(t = 0)$ is a mock cover. Then every finite group generated by elements whose orders lie in S occurs as the Galois group of a regular Galois extension of $A[[t]]$.*

Proof. Let $g_1,..., g_n$ be generators of G, say, of orders $n_1,..., n_m \in S$. Let H_i be the cyclic group generated by g_i. We may inductively define (for $1 \leqslant i \leqslant m$) non-zero elements $h_i, g_i \in A$ and Galois cyclic degree n_i covers $Y_i \to \operatorname{Spec} A[h_i^{-1}][[t]]$ whose fibre over $(t = 0)$ is a mock cover with branch locus (g_i), such that $h_i = \prod_{j<i} g_j$ and such that g_i is relatively prime to h_i. Let $f_i = \prod_{j \neq i} g_j$, let $U_i = \operatorname{Spec} A[f_i^{-1}]$, and let Z_i be the pullback of Y_i to $\operatorname{Spec} A[f_i^{-1}][[t]]$. On the closed fibre of the normalization of Y_i, the stabilizers of the ramification points on the identity sheet generate H_i (by

1.1), and all these points lie over U_i. So the normalization of Z_i is connected. Thus Z_i is irreducible, and hence a cyclic Galois cover branched only over U_i, though not over $U_i \cap U_j$ (for $j \neq i$). By construction, $f_1,...,f_m$ generate the unit ideal. Thus 1.2 applies, and yields a Galois cover of Spec $A[[t]]$ with group G, and whose fibre over $(t=0)$ is a mock cover. ∎

1.4. COROLLARY. *Let k be a field containing primitive nth roots of unity, for all n. (Of necessity,* char $k = 0$.) *Then every finite group occurs as the Galois group of a Galois regular extension of $k[x][[t]]$.*

Proof. This follows from Corollary 1.3, using cyclic extensions of the form

$$z^n = \alpha^{n-1}(\alpha - t).$$

Here $\alpha \in k$ is chosen not to be a pth power, for any prime $p \mid n$. ∎

Alternatively, to vary the branch locus and obtain new extensions, one could use patches of the form $z^n = \alpha^{n-1}(\alpha - tf(t))$; here $f(t) \in k[t]$.

Actually, the existence of nth roots of unity is not essential. In characteristic p, for example, there are no primitive pth roots of unity, but we still have

1.5. COROLLARY. *Let k be an algebraically closed field of characteristic p. Then every finite group occurs as the Galois group of a regular Galois extension of $k[x][[t]]$, and also as a Galois group over $k[x]$.*

Proof. In order to apply Corollary 1.3, observe that every finite group is generated by elements of order prime to p and elements whose order is a power of p. If n is prime to p then k has a primitive nth root of unity; then use an extension as in 1.4. For powers of p, we may use Witt vectors: Let $W = W_r(k[x][[t]][z_0,..., z_{r-1}])$ be the truncated Witt ring of degree r, and let F be the Frobenius endomorphism of W. Then a cyclic extension of degree p^r is given by the Witt coordinates of $F(z) - \alpha^{p-1}z - t = 0$; here $\alpha \in k[x]$ is a non-zero non-unit, and $\alpha, z \in W$ are the Witt vectors with Witt coordinates $(\alpha, 0,..., 0)$ and $(z_0,..., z_{r-1})$, respectively. (The generator of $\mathbb{Z}/p^r$ acts by $z \mapsto z + \alpha$, and the fibre over $(t=0)$ is a mock cover.) By 1.3, this yields the first assertion.

By the remark after 1.2, G occurs over $R[x]$ for some étale extension $k[t] \subset R$. Since k is algebraically closed, we may specialize to a closed point of Spec R without extension of constants. Thus G occurs over $k[x]$. ∎

Again, there was a great deal of freedom in the construction: in choosing the generators, the branch points, the elements α, and (when passing to $k[x]$) the point of specialization. Moreover, by instead using $F(z) - f(x,t)^{p-1}z - t = 0$, the branch locus can be varied.

On the other hand, with the construction as in 1.5, using specialization we obtain

1.6. COROLLARY. *Let k be an algebraically closed field of characteristic p, let $\xi_1,\dots,\xi_m \in k$ be distinct elements, and let G be a finite group generated by m elements of order p. Then there are (infinitely many) Galois covers of $\mathbb{A}^1_k$ with group G, branched precisely at $\xi_1,\dots,\xi_m \in \mathbb{A}^1$, and with p-fold ramification at each of these points.*

Moreover, this remains true if one more generally considers groups G generated by m p-groups $H_1,\dots,H_m \subset G$, if in the conclusion one allows p-power ramification over each ξ_i. This follows by replacing the Witt vector construction by Theorem 1.2 of [Ha2], in order to obtain a family of covers with a given p-group as Galois group, and totally ramified over a given $(x=\xi)$.

Observe also that the proofs of 1.4–1.6 still hold if $k[x]$ is replaced by $R[f^{-1}]$, for some finite extension R of $k[x]$—i.e., if curves other than the affine line are considered.

Proposition 1.2 and Corollary 1.3 can also be applied in the mixed characteristic case, and we study this in Section 2.

2. THE ARITHMETIC CASE

Using the ideas of Section 1, we show how to construct Galois extensions of arithmetic power series rings, using mock covers.

2.1. PROPOSITION. *Let $\mathcal{O}$ be the ring of integers in a number field which contains a primitive nth root of unity. Let G be a finite group generated by elements $d_1,\dots,d_m$ of orders $n_1,\dots,n_m$, where each $n_i \mid n$. Let $h_1,\dots,h_m \in \mathcal{O}[t]$, such that h_i is not divisible by a pth power for any prime $p \mid n_i$, and such that $h_i(0) = a_i^{n_i}$, for some non-unit $a_i \in \mathcal{O}$ which is relatively prime to $n\prod_{j\neq i} a_j$. Then there is a regular Galois cover of* Spec $\mathcal{O}[[t]]$ *with group G, ramified precisely over $h_1,\dots,h_m$, with ramification indices $n_1,\dots,n_m$, and whose closed fibre is a mock cover.*

Proof. Let $e_0 = a_1 a_2 \cdots a_n$, $h_0 = 1$, $n_0 = 1$. For $1 \leqslant i \leqslant m$ let $e_i = n\prod_{j\neq i} h_j(0)$. Thus $e_0,\dots,e_n$ generate the unit ideal. For all i, let $\mathcal{O}_i = \mathcal{O}[e_i^{-1}]$. The cover $Z \to \text{Spec}\,\mathcal{O}_i[[t]]$ given by $z^{n_i} = h_i$ is a Galois n_i-cyclic cover, whose fibre over $(t=0)$ is a connected mock cover. Applying Proposition 1.2 yields the desired cover. ∎

Since every simple group is generated by involutions (inasmuch as the subgroup so generated is normal and nontrivial), the construction in 2.1

yields Galois covers with any such group, regardless of which number field is considered.

If the assumption on nth roots of unity is dropped, a given group can still be realized as a Galois group, though with less control over the branch locus. In order to deduce this using Section 1, we first show the following result, which relies on ideas of [Sa].

2.2. PROPOSITION. *Let p be a prime number and n a positive integer. Then for infinitely many primes q, there is a domain S which is a finite free $\mathbb{Z}[t]$-algebra, Galois and cyclic of order p^n, such that*

(i) *the analytic space associated to S is unramified over the open unit t-disc,*

(ii) Spec $S/(t) \to$ Spec $\mathbb{Z}$ *is a connected Galois mock cover which is unramified except at q (where it is totally ramified), and*

(iii) Spec S *is locally irreducible at every point of* Spec $S/(t)$.

Of course for finite $\mathbb{Z}[t]$-algebras, being free is equivalent to being flat.

Proof. Recall that if A is an integrally closed domain containing a primitive pth root of unity ζ_p, and $a \in A$, then the integral closure B of $A[a^{1/p}]$ is a cyclic extension, étale at $\mathfrak{p} \in \text{Spec } A$ if $p \in \mathfrak{p}$ and $a \equiv 1 \pmod{\mathfrak{p}^p}$. In particular, since $p \in \mathfrak{p}^{p-1}$, B is unramified over A at $\mathfrak{p}$ provided $a \equiv 1 \pmod{p^2}$. More generally, if A contains ζ_{p^r}, and $a \equiv 1 \pmod{p^2}$, then the integral closure of $A[a^{1/p^r}]$ is also cyclic, and étale over any prime $\mathfrak{p}$ containing p, since the extension $A[a^{1/p^i}] \subset A[a^{1/p^{i+1}}]$ is obtained by adjoining the pth root of an element congruent to 1 modulo p^2. Namely, if a^{1/p^i} has (inductively) been chosen to be congruent to 1 modulo p^2, then any pth root of a^{1/p^i} is congruent to 1 modulo p. Since the pth roots of unity form a complete set of residues modulo p^2 for the elements congruent to 1 modulo p, it follows that some pth root of a^{1/p^i} is congruent to 1 modulo p^2.

We now consider separate cases:

Case I: $p \neq 2$. Let q be any prime which is congruent to 1 modulo p^2. The group of units in $\mathbb{Z}/p^n$ is a cyclic group of order $s = p^{n-1}(p-1)$; let m be a generator. The ring $R = \mathbb{Z}[\zeta_{p^n}]$ is Galois and cyclic over $\mathbb{Z}$ of degree s, and $\tau: \zeta_{p^n} \mapsto \zeta_{p^n}^m$ is a generator of its Galois group. This extends to an action on $R[t]$ over $\mathbb{Z}[t]$. By construction $m^s \equiv 1 \pmod{p^n}$, so $m^s - p^n k = 1$ for some integer k. For any $a \in R[t]$ define (following Theorem 2.3 of [Sa])

$$M(a) = a^{m^{s-1}} \tau(a)^{m^{s-2}} \cdots \tau^{s-2}(a)^m \tau^{s-1}(a).$$

Thus

$$M(aa') = M(a)\, M(a')$$

and

$$\begin{aligned} M(a)^m a^{-kp^n} &= a^{m^s}\tau(a)^{m^{s-1}} \cdots \tau^{s-1}(a)^m a^{-kp^n} \\ &= \tau(a)^{m^{s-1}} \tau^2(a)^{m^{s-2}} \cdots \tau^{s-1}(a)^m a \\ &= \tau(M(a)). \end{aligned}$$

Let $b(t) = q^{p^n} + p^2\zeta_{p^n} t \in R[t]$, define the domain

$$S_0' = R[t, y]/(y^{p^n} - M(b)),$$

and let S' be the integral closure of S_0'.

The extension $R[t] \subset S'$ is Galois and cyclic of order p^n, with generator $\sigma: y \mapsto \zeta_{p^n} y$. Since $M(b) \equiv 1 \pmod{p^2}$, it follows that $R[t] \subset S'$ is unramified over (P), where $P \in R$ is the prime lying over $p \in \mathbb{Z}$. Since the elements $\tau^i(b)$ generate distinct prime ideals in $R[t]$ for $i = 0, 1, \ldots, s-1$, it follows by Purity of Branch Locus [Na, 41.1] that $R[t] \subset S'$ is ramified precisely over the union of their loci—and in particular not at (P, t). Observe that Spec $S_0'/(t)$ and Spec $S'/(t)$ define p^n-cyclic mock covers of Spec R, and that Spec $S'/(t) \to$ Spec R is ramified precisely over q, where it is totally ramified. Also, $\mathbb{Z}[t] \subset S'$ is ramified precisely over $g(t) = \prod_{i=0}^{s-1} \tau^i(b)$ and over p. Here $g(t)$ is irreducible in $\mathbb{Z}[t]$ since it splits into a product of distinct irreducible conjugates in $\mathbb{Z}[\zeta_{p^n}, t]$. Also, $g(t)$ does not vanish in $|t| < 1$.

Now the action of τ on $R[t]$ over $\mathbb{Z}[t]$ extends to an action on frac S' over $\mathbb{Q}(t)$. Namely, since

$$(y^m b^{-k})^{p^n} = M(b)^m b^{-kp^n} = \tau(M(b)) = \tau(y^{p^n}) \in \text{frac } S',$$

there is a well-defined $\mathbb{Q}(t)$-algebra automorphism of frac S' which extends $\tau: R[t] \to R[t]$ and satisfies

$$\tau(y) = y^m b^{-k}.$$

Here τ remains of order s, since

$$\tau^s(y) = y^{m^s} M(b)^{-k} = y.$$

Since $y^m b^{-k} \in \text{frac } S'$ satisfies the monic polynomial $X^{p^n} - \tau(M(b))$ over $R[t]$, $y^m b^{-k}$ lies in the integrally closed domain S'. So τ restricts to an automorphism of S' over $\mathbb{Z}[t]$, of order s. Now

$$\sigma\tau(y) = \sigma(y^m b^{-k}) = \zeta_{p^n}^m y^m b^{-k} = \tau(\zeta_{p^n} y) = \tau\sigma(y),$$

so σ commutes with τ. Thus σ and τ generate an abelian group G of automorphisms of S' over $\mathbb{Z}[t]$. Since σ fixes $R[t]$, no $\sigma^i\tau^j = 1$ for $0 \leqslant i < p^n$, $0 \leqslant j < s$, except $(i, j) = (0, 0)$. So G is the product of a cyclic group of order

p^n with one of order s. Since S' is of degree $p^n s$ over $\mathbb{Z}[t]$, this makes S' into a G-Galois extension of $\mathbb{Z}[t]$. So $\mathbb{Z}[t]$ is the fixed ring of G.

Let $\phi_0' : S_0' \to R$ be the R-algebra homomorphism given by

$$t \mapsto 0, \qquad y \mapsto M(q) = q^{1+m+\cdots+m^{s-1}}.$$

This extends to a homomorphism $\phi' : S' \to R$ since S' is integral over S_0' and R is integrally closed. Then

$$\phi'(\tau(y)) = \phi'(y^m b^{-k}) = q^{m+m^2+\cdots+m^s-kp^n} = q^{1+m+\cdots+m^{s-1}} = \phi'(y)$$

using $m^s - kp^n = 1$. So $\phi' \circ \tau = \phi'$, and $\phi'(\tau^i(y)) = \phi'(y)$.

Let $x = y + \tau(y) + \cdots + \tau^{s-1}(y) \in S'$. Then for $0 \leqslant j < p^n$,

$$\begin{aligned}
\phi'(\sigma^j(x)) &= \sum_{i=0}^{s-1} \phi'(\tau^i \sigma^j(y)) \\
&= \sum_{i=0}^{s-1} \phi'(\tau^i(\zeta_{p^n}^j y)) \\
&= \sum_{i=0}^{s-1} \phi'(\zeta_{p^n}^{mj} \tau^i(y)) \\
&= \sum_{i=0}^{s-1} \zeta_{p^n}^{mj} q^{1+\cdots+m^{s-1}}.
\end{aligned}$$

So $\phi'(\sigma^j(x)) = s q^{1+\cdots+m^{s-1}}$ if and only if $j = 0$. Thus $\sigma^j(x) \neq x$ for $1 \leqslant j < p^n$, and hence $\sigma^i(x) \neq \sigma^j(x)$ for $0 \leqslant i < j < p^n$. Let $s_1, \ldots, s_{p^n}$ be the elementary symmetric polynomials in $x, \sigma(x), \ldots, \sigma^{p^n-1}(x)$. The s_i are invariant under σ, and also under τ since x is and $\sigma\tau = \tau\sigma$. Thus each $s_i \in \mathbb{Z}[t]$. Let

$$S_0 = \mathbb{Z}[t, X]/(X^{p^n} - s_1 X^{p^n-1} + s_2 X^{p^n-2} - \cdots + s_{p^n-1} X - s_{p^n}).$$

The defining polynomial is irreducible over $\mathbb{Z}[t]$ and splits over S', since its roots are the elements $\sigma^j(x) \in S'$, which are distinct and are conjugate over $\mathbb{Z}[t]$. Thus S_0 is a domain. Identifying $X = x$, $\mathbb{Q}(t) \subset \operatorname{frac} S_0$ is a Galois subextension of $\mathbb{Q}(t) \subset \operatorname{frac} S'$, cyclic of order p^n with group generator σ.

The integral closure S of S_0 is a finite $\mathbb{Z}[t]$-module, and its spectrum is locally irreducible at every point. The restriction of σ is an automorphism of S, so S is Galois and cyclic of order p^n over $\mathbb{Z}[t]$. Moreover S is flat. To see this, let $\mathfrak{m}$ be a maximal ideal of $\mathbb{Z}[t]$, let A be the localization of $\mathbb{Z}[t]$ at $\mathfrak{m}$, and let $B = A \otimes_{\mathbb{Z}[t]} S$. By [AB],

$$\text{projective dim}_A B + \text{depth}_A B = \text{depth } A.$$

But B is Cohen–Macaulay since it is normal and of dimension 2. So both depths equal 2, and thus B is a free A-module. Hence S is a flat (in fact free) $\mathbb{Z}[t]$-module.

Since frac S is the fixed field of frac S' under τ, it follows that frac S' is the compositum of frac$(R[t])$ and frac S over $\mathbb{Q}(t)$. Since $\mathbb{Q}(t) \subset \text{frac}(R[t])$ is Galois and $\text{frac}(R[t]) \cap \text{frac } S = \mathbb{Q}(t)$, it follows by Galois theory that actually $\text{frac}(R[t]) \otimes_{\mathbb{Q}(t)} \text{frac } S = \text{frac } S'$. Thus $R[t] \otimes_{\mathbb{Z}[t]} S \subset S'$, as S' is integrally closed. Hence $\mathbb{Z} \subset S/(t)$ is totally ramified at q, and so Spec $S/(t)$ is connected. Since S is integrally closed and $\mathbb{Z} \subset R$ is unramified except at p, it follows that $R[t] \otimes_{\mathbb{Z}[t]} S[p^{-1}] = S'[p^{-1}]$. Thus $S[p^{-1}, g^{-1}]$ is unramified over $\mathbb{Z}[p^{-1}, t, g^{-1}]$, and hence the analytic space associated to S is unramified over the open unit t-disc. It also follows that Spec $S/(t) \to$ Spec $\mathbb{Z}$ is a Galois cover, cyclic of order p^n, since it is a generically separable fibre of a cyclic Galois cover.

In fact Spec $S/(t) \to$ Spec $\mathbb{Z}$ is a mock cover. To see this, let ϕ' be as above and let $\phi = \phi' \restriction S$. Since $\phi(x) \in \mathbb{Z}$ and S is integral over S_0, we have $\phi: S \to \mathbb{Z}$. Thus Spec $S \to$ Spec $\mathbb{Z}[t]$ has a section over $(t = 0)$. Being Galois, its fibre over $(t = 0)$ is thus a mock cover.

It remains to show that $\mathbb{Z}[t] \subset S$ is unramified on $(t = 0)$ except at q. For this it suffices to prove the following:

Claim. S is étale over (p, t).

We conclude Case I by proving the claim. Let $S_p = \mathbb{Z}[t]_{(p,t)} \otimes_{\mathbb{Z}[t]} S$ and $S'_p = R[t]_{(P,t)} \otimes_{R[t]} S'$, where $P \mid p$ as above. We wish to show that S_p is étale over (p, t). Note first that $\mathbb{Z}[\zeta_p, t]$ is of degree $p - 1$ over $\mathbb{Z}[t]$, while any ramification of the Galois extension $\mathbb{Z}[t]_{(p,t)} \subset S_p$ has degree a power of p. So it suffices to show that the extension $\mathbb{Z}_{(p)}[\zeta_p, t] \subset S_p[\zeta_p]$ becomes unramified over (p, t) after passage to the integral closure. Let $\hat{\mathcal{O}}$ be the completion of $\mathbb{Z}_{(p)}[\zeta_p][[t]]$ at its maximal ideal, and let Spec $\hat{A}$ be the normalization of an irreducible component of Spec$(\hat{\mathcal{O}} \otimes_{\mathbb{Z}[\zeta_p, t]} S_p[\zeta_p])$. It suffices to show that $\hat{A} = \hat{\mathcal{O}}$, for then the integral closure of $S_p[\zeta_p]$ is indeed unramified at the prime over (p, t), and so S_p is unramified at (p, t).

We conclude the proof of the claim, and of Case I, by showing $\hat{A} = \hat{\mathcal{O}}$. The normalization of $\hat{A} \otimes_{\mathbb{Z}[\zeta_p, t]} R[t]$ is a direct product of copies of $\hat{\mathcal{O}}[\zeta_{p^n}]$, inasmuch as S'_p is unramified over (P, t) and has no residue field extension there. So $\hat{\mathcal{O}} \subset \hat{A} \subset \hat{\mathcal{O}}[\zeta_{p^i}]$. Since $\hat{A}$ and $\hat{\mathcal{O}}[\zeta_{p^n}]$ (for $1 \leqslant i \leqslant n$) are integrally closed, and since the extension $\hat{\mathcal{O}} \subset \hat{\mathcal{O}}[\zeta_{p^n}]$ is cyclic of order p^{n-1}, it follows that $\hat{A} = \hat{\mathcal{O}}[\zeta_{p^i}]$ for some $1 \leqslant i \leqslant n$. If $i > 1$ then the integral closure of $\hat{\mathcal{O}}/(t) \subset \hat{A}/(t)$ is ramified over the maximal ideal $\hat{p}$. But since the normalization of a mock cover is unramified, this is not the case. So actually $i = 1$, and $\hat{A} = \hat{\mathcal{O}}$ as desired.

Case II: $p = 2$.

Subcase (a): $n = 1$, $p^n = 2$. Let q be any prime number other than 2, and let $S = \mathbb{Z}[t, y]/(y^2 - qy + t)$. Then S is a domain, free over $\mathbb{Z}[t]$, and ramified precisely over $g(t) = q^2 - 4t$, which does not vanish in $|t| < 1$. Also, Spec $S/(t) \to$ Spec Z is a mock cover ramified precisely over q, where it is totally ramified and locally irreducible. So S is as desired.

Subcase (b): $n = 2$, $p^n = 4$. Let $q > 0$ be any prime congruent to 1 modulo 4. The ring $\mathbb{Z}[i]$ is Galois and cyclic over $\mathbb{Z}$ of degree 2, the generator κ of the Galois group being complex conjugation. This extends to an action of $\mathbb{Z}[i, t]$ over $\mathbb{Z}[t]$. Proceeding parallel to Case I, we define (folowing Theorem 2.4 of [Sa]) the domain

$$S_0' = \mathbb{Z}[i, t, y]/(y^4 - (q + 4it)^3(q - 4it)),$$

and we let S' be the integral closure of S_0'. Then S' is Galois over $\mathbb{Z}[i, t]$ and cyclic of order 4, with generator $\sigma: y \to iy$. Since $(q + 4it)^3(q - 4it) \equiv 1 \pmod 4$, it follows that $\mathbb{Z}[i, t] \subset S'$ is unramified over $(1 + i)$, the prime in $\mathbb{Z}[i]$ over 2. Thus $\mathbb{Z}[i, t] \subset S'$ is ramified precisely over the union of the loci of $b = q + 4it$ and of $\kappa(b) = q - 4it$, so is unramified at $(1 + i, t)$. The spectrum of the residue modulo t is a cyclic Galois mock cover of degree 4, totally ramified over q. Also, $\mathbb{Z}[t] \subset S'$ is ramified precisely over (2) and over the locus of the polynomial $g(t) = b\kappa(b) = q^2 + 16t^2$, which is irreducible in $\mathbb{Z}[t]$.

Now the action of κ on $\mathbb{Z}[i, t]$ over $\mathbb{Z}[t]$ extends to an action of frac S' over $\mathbb{Q}(t)$. Namely, since

$$(y^{-1}g)^4 = b^{-3}\kappa(b)^{-1}\, g^4 = \kappa(b^3\kappa(b)) = \kappa(y^4),$$

there is a well-defined $\mathbb{Q}(t)$-algebra automorphism κ of frac S' which extends $\kappa: \mathbb{Z}[i, t] \to \mathbb{Z}[i, t]$ and satisfies $\kappa(y) = y^{-1}g$. Here κ remains an involution since $\kappa^2(y) = \kappa(y^{-1}g) = y$. Since $y^{-1}g \in$ frac S' satisfies the monic polynomial $X^4 - b^3\kappa(b)$ over $\mathbb{Z}[i, t]$, $y^{-1}g$ lies in the integrally closed domain S'. So κ restricts to an automorphism of S' over $\mathbb{Z}[t]$, of order 2. Now

$$\sigma\kappa(y) = \sigma(y^{-1}g) = -iy^{-1}g = \kappa(iy) = \kappa\sigma(y),$$

so σ and κ commute. Thus σ and κ generate a group of automorphisms of S' over $\mathbb{Z}[t]$, isomorphic to the product of a cyclic group of order 4 with one of order 2. This makes S' into a Galois extension of $\mathbb{Z}[t]$ with this group.

The remainder of the construction is just as in Case I.

Subcase (c): $n > 2$. Let $q > 0$ be any prime congruent to 1 modulo 4. The ring $R = \mathbb{Z}[\zeta_{2^n}]$ is Galois over $\mathbb{Z}$, and its group is the product of a cyclic group of order $s = 2^{n-2}$ and a cyclic group of order 2. The generator of the former is $\tau: \zeta_{2^n} \to \zeta_{2^n}^5$, and the generator κ of the latter is complex

conjugation. These extend to actions of $R[t]$ over $\mathbb{Z}[t]$. Since 5 has order s in the group of units in $\mathbb{Z}/2^n$, $5^s - 2^n k = 1$ for some integer k. Let $b(t) = q^{2^n} + 4\zeta_{2^n} t \in R[t]$ and $a = b^{2^{n-1}+1} \kappa(b)^{2^{n-1}-1}$. In the notation of Case I with $m = 5$ (and following Theorem 2.7 of [Sa]), define the domain

$$S_0' = R[t, y]/(y^{2^n} - M(a)),$$

and let S' be the integral closure of S_0'.

As in Cases I and II(b), S' is Galois over $R[t]$, cyclic of order 2^n, with generator $\sigma: y \mapsto \zeta_{2^n} y$. The extension $R[t] \subset S'$ is ramified precisely over the locus of $M(a)$, and the spectrum of its residue modulo t is a cyclic mock cover, ramified only at q, where it is totally ramified. Also, $\mathbb{Z}[t] \subset S'$ is ramified precisely over (2) and the locus of the irreducible polynomial $g = \prod_{i=0}^{1} \prod_{j=0}^{s-1} \kappa^i \tau^j(b) \in \mathbb{Z}[t]$.

Now the actions of τ and κ on $R[t]$, over $\mathbb{Z}[i, t]$ and $\mathbb{Z}[\zeta_{2^n} + \zeta_{2^n}^{-1}, t]$, respectively, extend to actions on frac S'. Namely, since

$$(y^5 a^{-k})^{2^n} = M(a)^5 a^{-2^n k} = \tau(M(a))$$

using the identity established in the proof of Case I, there is a well-defined $Q(i, t)$-algebra automorphism τ of frac S' which extends the original τ and satisfies $\tau(y) = y^5 a^{-k}$. Using the fact that $\kappa\tau = \tau\kappa$,

$$M(a)\,\kappa(M(a)) = M(a)\,M(\kappa(a)) = M(a\kappa(a)) = M(b^{2^n}\kappa(b)^{2^n});$$

so there is a well-defined $Q(\zeta_{2^n} + \zeta_{2^n}^{-1}, t)$-algebra automorphism κ of frac S' which extends the original κ and satisfies $\kappa(y) = y^{-1} M(b\kappa(b))$. By the same computations as in Cases I and II(b), τ and κ remain of orders 5 and 2, respectively. Since $y^5 a^{-k}$ and $y^{-1} M(b\kappa(b))$ satisfy the monic polynomials $X^{2^n} - M(a)^5 a^{-2^n k}$ and $X^{2^n} - \kappa(M(a))$, respectively, they each lie in S', and so τ and κ restrict to automorphisms of S'. Together with σ, they generate a group of automorphisms of S' over $\mathbb{Z}[t]$, viz., the full Galois group.

The remainder of the construction is as in Case I. ∎

Using this, we obtain the desired

2.3. PROPOSITION. *Let $\mathcal{O}$ be the ring of integers in a number field, and G a finite group. Then G occurs as the Galois group of a regular Galois extension of $\mathcal{O}[[t]]$.*

Proof. For $\mathcal{O} = \mathbb{Z}$, this follows from Proposition 2.2 and Corollary 1.3, since every group is generated by elements of prime power order. For other rings $\mathcal{O}$, observe that $\mathbb{Z} \subset \mathcal{O}$ is ramified only at finitely many primes p_i, and that a pullback of a connected mock cover of Spec $\mathbb{Z}$ is a connected mock cover of Spec $\mathcal{O}$. So a desired Galois $\mathcal{O}[[t]]$-algebra may be constructed by first using 1.3 to construct a Galois extension of $\mathbb{Z}[[t]]$ with group G which

is unramified at the primes p_i, and then tensoring over $\mathbb{Z}[[t]]$ with $\mathcal{O}[[t]]$. ∎

Condition (i) in Proposition 2.2 allows us to descend the extension in 2.3 somewhat. As in [Ha3], for $r>0$ let $\mathbb{C}_{r+}[[t]]$ be the subring of $\mathbb{C}[[t]]$ consisting of power series with radius of convergence greater than r. For $A \subset \mathbb{C}$ let $A_{r+}[[t]] = A[[t]] \cap \mathbb{C}_{r+}[[t]]$. If $r \geqslant 1$ then $\mathbb{Z}_{r+}[[t]] = \mathbb{Z}[t]$, while for $0<r<1$ the rings $\mathbb{Z}_{r+}[[t]]$ "interpolate" between the convergent power series ring and the polynomial ring. According to Corollary 2.9 of [Ha3], if $0<r<1$ and $A, B \subset \mathbb{Q}$ satisfy $A \cap B = \mathbb{Z}$, then given free algebras over $A[[t]]$ and $B_{r+}[[t]]$ which are G-Galois and agree over $AB[[t]]$, there is a unique free $\mathbb{Z}_{r+}[[t]]$-algebra which is G-Galois and induces both of them, compatibly.

2.4. PROPOSITION. *If G is a finite group and $0<r<1$, then G occurs as the Galois group of a regular Galois extension of $\mathbb{Z}_{r+}[[t]]$.*

Actually, we will show more, including that the extension may be chosen to be regular, and also "purely arithmetic" (i.e., the corresponding extension of analytic spaces is trivial). Namely, we show, for any choice of r and G,

2.4′. *Claim.* There is a finite free Galois $\mathbb{Z}_{r+}[[t]]$-algebra R with group G, whose associated complex analytic space is unramified over $|t| \leqslant r$, and whose reduction modulo t defines a connected mock cover, at every point of which Spec R is locally irreducible.

Proof of 2.4′ (and hence of 2.4). Let $d_1, \ldots, d_m$ be a generating set for G, and $N = \#G$. We may assume that each d_i has prime power order, say, $p_i^{v_i}$. We prove the claim by induction on m. If $m=1$ this follows immediately from Proposition 2.2. Assume the claim for $m-1$. Let $H \subset G$ be the subgroup generated by $\{d_1, \ldots, d_{m-1}\}$, and write $d = d_m$, $p = p_m$, $v = v_m$. Let h be the index of H in G. By the inductive hypothesis, there is an H-algebra R_2^0 over $\mathbb{Z}_{r+}[[t]]$ having the properties asserted in the claim. Thus $R_2^0/(t)$ is étale away from (a), for some $a \in \mathbb{Z}^+$. Let R_1^0 be the p^n-cyclic extension of $\mathbb{Z}[t]$ guaranteed by Proposition 2.2 applied to p and v, with q chosen prime to a. Let $R_1 = R_1^0 \otimes_{\mathbb{Z}[t]} \mathbb{Z}_{(q)}[[t]]$ and $R_2 = R_2^0 \otimes_{\mathbb{Z}_{r+}[[t]]} \mathbb{Z}[q^{-1}]_{r+}[[t]]$. Then R_1^{N/p^n} and R_2^h are G-extensions of $\mathbb{Z}_{(q)}[[t]]$ and $\mathbb{Z}[q^{-1}]_{r+}[[t]]$, whose spectra are locally irreducible and whose fibres over $(t=0)$ are mock covers. Moreover they are free as algebras. By Corollary 2.9 of [Ha3], they patch to form a free G-Galois $\mathbb{Z}_{r+}[[t]]$-algebra R. Now Spec $R \to$ Spec $\mathbb{Z}_{r+}[[t]]$ is locally irreducible along $(t=0)$, has a connected mock cover as its fibre over $(t=0)$, and is analytically unramified over $|t| \leqslant r$. Thus $R \otimes_{\mathbb{Z}_{r+}[[t]]} \mathbb{Z}[[t]]$ is a domain. But this domain includes R, using that R is flat over $\mathbb{Z}_{r+}[[t]]$. Thus R is a domain, and hence Spec $R \to$ Spec $\mathbb{Z}_{r+}[[t]]$ is Galois, as desired. ∎

REFERENCES

[AB] M. AUSLANDER AND D. BUCHSBAUM, Homological dimension in local rings, *Trans. Amer. Math. Soc.* **85** (1957), 390–405.

[Ha1] D. HARBATER, Deformation theory and the tame fundamental group, *Trans. Amer. Math. Soc.* **262** (1980), 399–415.

[Ha2] D. HARBATER, Moduli of p-covers of curves, *Comm. Algebra* **8** (12) (1980), 1095–1122.

[Ha3] D. HARBATER, Convergent arithmetic power series, *Amer. J. Math.* **106** (1984), 801–846.

[Na] M. NAGATA, "Local rings," Interscience, New York, 1962.

[Sa] D. SALTMAN, Generic galois extensions and problems in field theory, *Adv. in Math.* **43** (3) (1982), 250–283.